



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/718,369	11/19/2003	Sundeep M. Bajikar	1020.P17644	9547

⁷⁵⁹⁰
Kacvinsky LLC
c/o Intellevate
P.O. Box 52050
Minneapolis, MN 55402

EXAMINER

TO, BAOTRAN N

ART UNIT	PAPER NUMBER
----------	--------------

2435

MAIL DATE	DELIVERY MODE
-----------	---------------

01/23/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/718,369	Applicant(s) BAJIKAR ET AL.	
	Examiner Bao tran N. To	Art Unit 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10/23/2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This Office action is in response to Applicant's Amendment filed 10/23/2008.
Claims 1, 5, 11, 16, and 20 are amended.
Claims 1-29 are pending in the application.

Response to Arguments

2. Applicant's arguments filed 10/23/2008 have been fully considered but they are not persuasive.

Applicant appears to argue that "Gregg fails to teach or suggest a method of establishing a protected communications channel with a trusted code module executing in a trusted execution environment in an open platform of a computing system, as recited by amended independent claims 1 and 11" (Page 10 of Remarks).

This argument is no persuasive because Claims 1 and 11 are rejected under 103 as being unpatentable over Kalavade and Gregg. Kalavade expressly discloses establishing a protected communications channel (SSL) with a computing system (Figure 12, paragraph 0236), but does not disclose a trusted code module executing in a trusted environment in an open platform of a computer system. However, Gregg expressly discloses a trusted code module executing in a trusted environment in an open platform of a computer system (Figure 25, paragraphs 0099-0101). Accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Gregg's invention within Kalavade to include a trusted code module executing in a trusted environment in an open platform of a computer system.

One of ordinary skill in the art would have been motivated to do this because it would provide enhanced security. Therefore, the combination of Kalavade and Gregg discloses the limitations of Claims 1 and 11.

Applicant further argues with respect to independent claim 5 that Gregg also fails to teach or suggest "establishing a protected communications channel with a trusted code module executing in a protected execution environment in an open platform of a computing system; using subscriber identity module (SIM) capabilities provided by the computing system in the protected execution environment without a discrete hardware SIM device for user authorization, authentication and accounting in association with a subscription account; and providing a subscription account service for access by the open platform of the computing system using the SIM capabilities in the protected execution environment of the computing system" (Page 11 of Remarks).

This argument is no persuasive because Claim 5 is rejected under 103 as being unpatentable over Kalavade and Gregg. Kalavade expressly discloses establishing a protected communications channel (SSL) with a computing system (Figure 12, paragraph 0236); using subscriber identity module (SIM) capabilities provided by a computing system without a discrete hardware SIM device for user authorization (paragraphs 0103 and 0110-0111), authentication and accounting in association with a subscription account (paragraph 0063); and providing a subscription account service for access by the computing system (paragraph 0180), but does not disclose a trusted code module executing in a protected environment in an open platform of a computer

Art Unit: 2435

system and providing access to a trusted environment in an open platform. However, Gregg expressly discloses a trusted code module executing in a trusted environment in an open platform of a computer system and providing access to a trusted environment in an open platform (Figure 25, paragraphs 0099-0101). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Gregg's invention within Kalavade to include a trusted code module executing in a trusted environment in an open platform of a computer system and providing access to a trusted environment in an open platform. One of ordinary skill in the art would have been motivated to do this because it would provide enhanced security.

Applicant further argues with respect to independent claim 16 that Gregg also fails to teach or suggest "establishing a protected communications channel with a trusted code module executing in a trusted execution environment in an open platform of a computing system; authenticating and authorizing a user of a subscription account at least in part by using Subscriber Identity Module (SIM) compliant authentication and authorization capabilities on a trusted execution environment in the open platform of the computing system that provides the SIM-compliant authentication and authorization capabilities without use of a discrete SIM hardware device; and providing user access to the subscription account upon receipt of predetermined credentials" (Page 11 of Remarks).

This argument is no persuasive because Claim 16 is rejected under 103 as being unpatentable over Kalavade and Gregg. Kalavade establishing a protected

communications channel (SSL) with a computing system (Figure 12, paragraph 0236); authenticating and authorizing a user of a subscription account at least in part by using Subscriber Identity Module (SIM) compliant authentication and authorization capabilities on a computing system that provides the SIM-compliant authentication and authorization capabilities without use of a discrete SIM hardware device (paragraphs 0103 and 0110-0111); and providing user access to the subscription account upon receipt of predetermined credentials (paragraph 0103). Kalavade does not disclose a trusted code module executing in a protected environment in an open platform of a computer system. However, Gregg expressly discloses a trusted code module executing in a trusted environment in an open platform of a computer system (Figure 25, paragraphs 0099-0101). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Gregg's invention within Kalavade to include a trusted code module executing in a trusted environment in an open platform of a computer system. One of ordinary skill in the art would have been motivated to do this because it would provide enhanced security.

Applicant further argues with respect to independent claim 20 that Gregg also fails to teach or suggest "a provisioning module stored on the server, the provisioning module, when executed by the provisioning server, to establish a protected communications channel with a trusted module executing in a trusted execution environment in an open platform of a computing system and participate in provisioning Subscriber Identity Module (SIM) secret data from the server to the trusted execution

environment, the computing system to provide SIM-compliant authentication, authorization, and accounting capabilities without use of a discrete hardware SIM device, and the server to provide access to a service by the computing system using the SIM-compliant authentication, authorization and accounting capabilities in the trusted execution environment of the computing system" (Page 11 of Remarks).

This argument is no persuasive because Claim 20 is rejected under 103 as being unpatentable over Kalavade and Gregg. Kalavade discloses a server having access to a network (Figure 1, element 10); and a provisioning module stored on the server, the provisioning module, when executed by the provisioning server, to establishing a protected communications channel (SSL) with a computing system (Figure 12, paragraph 0236); participate in provisioning Subscriber Identity Module (SIM) secret data from the server to a computing system (Figures 1-3), the computing system to provide SIM-compliant authentication, authorization and accounting capabilities without use of a discrete hardware SIM device (paragraphs 0103 and 0110-0111). Kalavade does not disclose a trusted code module executing in a protected environment in an open platform of a computer system. However, Gregg expressly discloses a trusted code module executing in a trusted environment in an open platform of a computer system (Figure 25, paragraphs 0099-0101). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Gregg's invention within Kalavade to include a trusted code module executing in a trusted environment in an open platform of a computer system. One of ordinary skill in the art would have been motivated to do this because it would provide enhanced

security. Kalavade and Gregg disclose the limitations of Claim 20 above. Kalavade and Gregg further disclose the server (Figure 1, element 10) to provide access to a service by the computing system (Gregg, Figure 25, paragraphs 0099-010) using the SIM AAA capabilities (Kalavade paragraph 0103) in the trusted execution environment of the computing system (Gregg, Figure 25, paragraphs 0099-010).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Kalavade's reference and Gregg's reference are analogous arts. They both specifically disclose how to secure transactions and computer resources with untrusted network that can support the motivation to combine the Kalavade's teaching with Gregg's teaching to establish the limitations of Claim 1 that provides enhanced security.

For at least the above reasons, it is believed that the rejection is maintained.

Claim Objections

3. Claim 20 is objected to because of the following informalities: "the provisioning server" in line 4 should be ----the server----. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kalavade et al. (U.S. Patent Application Publication 2003/0051041 A1) hereinafter Kalavade in view of Gregg et al. (U.S. Patent Application Publication 2003/0046589 A1) hereinafter Gregg.

Regarding Claims 1 and 11, Kalavade discloses a method comprising:

establishing a protected communications channel (SSL) with a computing system (Figure 12, paragraph 0236), the computing system providing subscriber identity module (SIM) authentication, authorization, and accounting SIM AAA capabilities without use of a discrete hardware SIM device ("SIM module" paragraphs 0103 and 0110-0111), but does not disclose a trusted code module executing in a trusted environment in an open platform of a computer system and providing access to a trusted environment in an open platform.

However, Gregg expressly discloses a trusted code module executing in a trusted environment in an open platform of a computer system and providing access to a trusted environment in an open platform (Figure 25, paragraphs 0099-0101).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Gregg's invention within Kalavade to include a trusted code module executing in a trusted environment in an open platform of a computer system and providing access to a trusted environment in an open platform. One of ordinary skill in the art would have been motivated to do this because it would provide enhanced security.

Kalavade and Gregg disclose the limitations of Claims 1 and 11 above. Kalavade and Gregg further disclose provisioning SIM secret data (login/password information) to the computing system over the protected communications channel (Kalavade, paragraphs 0109- 0124 and 149).

providing access to a service by the open platform of the computing system (Gregg, Figure 25, paragraphs 0099-010) using the SIM AAA capabilities (Kalavade paragraph 0103) in the trusted execution environment of the computing system (Gregg, Figure 25, paragraphs 0099-010).

Regarding Claim 5, Kalavade discloses a method comprising:

establishing a protected communications channel (SSL) with a computing system (Figure 12, paragraph 0236);

using subscriber identity module (SIM) capabilities provided by a computing system without a discrete hardware SIM device for user authorization (paragraphs 0103 and 0110-0111), authentication and accounting in association with a subscription account (paragraph 0063); and

providing a subscription account service for access by the computing system (paragraph 0180), but does not disclose a trusted code module executing in a protected environment in an open platform of a computer system and providing access to a trusted environment in an open platform.

However, Gregg expressly discloses a trusted code module executing in a trusted environment in an open platform of a computer system and providing access to a trusted environment in an open platform (Figure 25, paragraphs 0099-0101).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Gregg's invention within Kalavade to include a trusted code module executing in a trusted environment in an open platform of a computer system and providing access to a trusted environment in an open platform. One of ordinary skill in the art would have been motivated to do this because it would provide enhanced security.

Regarding Claim 16, Kalavade discloses a method comprising:

establishing a protected communications channel (SSL) with a computing system (Figure 12, paragraph 0236);

authenticating and authorizing a user of a subscription account at least in part by using Subscriber Identity Module (SIM) compliant authentication and authorization capabilities on a computing system that provides the SIM-compliant authentication and authorization capabilities without use of a discrete SIM hardware device (paragraphs 0103 and 0110-0111); and

providing user access to the subscription account upon receipt of predetermined credentials (paragraph 0103).

Kalavade does not disclose a trusted code module executing in a protected environment in an open platform of a computer system.

However, Gregg expressly discloses a trusted code module executing in a trusted environment in an open platform of a computer system (Figure 25, paragraphs 0099-0101).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Gregg's invention within Kalavade to include a trusted code module executing in a trusted environment in an open platform of a computer system. One of ordinary skill in the art would have been motivated to do this because it would provide enhanced security.

Regarding Claim 20, Kalavade discloses an apparatus comprising:
a server having access to a network (Figure 1, element 10); and
a provisioning module stored on the server, the provisioning module, when executed by the provisioning server, to establishing a protected communications channel (SSL) with a computing system (Figure 12, paragraph 0236);

participate in provisioning Subscriber Identity Module (SIM) secret data from the server to a computing system (Figures 1-3), the computing system to provide SIM-compliant authentication, authorization and accounting capabilities without use of a discrete hardware SIM device (paragraphs 0103 and 0110-0111).

Kalavade does not disclose a trusted code module executing in a protected environment in an open platform of a computer system.

However, Gregg expressly discloses a trusted code module executing in a trusted environment in an open platform of a computer system (Figure 25, paragraphs 0099-0101).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Gregg's invention within Kalavade to include a trusted code module executing in a trusted environment in an open platform of a computer system. One of ordinary skill in the art would have been motivated to do this because it would provide enhanced security.

Kalavade and Gregg disclose the limitations of Claim 20 above. Kalavade and Gregg further disclose the server (Figure 1, element 10) to provide access to a service by the computing system (Gregg, Figure 25, paragraphs 0099-010) using the SIM AAA capabilities (Kalavade paragraph 0103) in the trusted execution environment of the computing system (Gregg, Figure 25, paragraphs 0099-010).

Regarding Claims 2 and 12, Kalavade and Gregg disclose the limitations of Claim 1 above. Kalavade further discloses wherein provisioning SIM secret data includes provisioning at least one of identity secrets, key secrets, information to initialize data objects, information to initialize operator-specific cryptography algorithms, and information to install or update applications, parameters, tools or utilities (paragraph 0409).

Regarding Claims 3 and 14, Kalavade and Gregg disclose the limitations of Claim 1 above. Kalavade further discloses wherein establishing a protected communications channel includes using a protected key exchange mechanism (paragraph 0236).

Regarding Claims 4 and 13, Kalavade and Gregg disclose the limitations of Claim 1 above. Kalavade further discloses wherein provisioning SIM secret data includes encrypting the SIM secret data (paragraph 0174).

Regarding Claim 6, Kalavade and Gregg disclose the limitations of Claim 5 above. Kalavade further discloses wherein providing the subscription account service includes providing a wireless network access account (paragraph 0176).

Regarding Claim 7, Kalavade and Gregg disclose the limitations of Claim 6 above. Kalavade further discloses wherein using SIM capabilities provided by a computing system includes using SIM capabilities provided by a laptop computing system (Figure 1, element 16).

Regarding Claim 8, Kalavade and Gregg disclose the limitations of Claim 5 above. Kalavade further discloses 5 wherein providing the subscription account service includes providing a wired network access account (paragraphs 0176 and 0444).

Regarding Claim 9, Kalavade and Gregg disclose the limitations of Claim 5 above. Kalavade further discloses wherein using SIM capabilities includes using the protected execution environment provided by a laptop computing system (paragraphs 0176 and 0277).

Regarding Claim 10, Kalavade and Gregg disclose the limitations of Claim 5 above. Kalavade further discloses wherein providing the subscription account service includes providing location-based services (paragraph 0364).

Regarding Claim 15, Kalavade and Gregg disclose the limitations of Claim 11 above. Kalavade further discloses wherein establishing a protected communications channel includes receiving authentication information from the computing system (paragraph 0410).

Regarding Claim 17, Kalavade and Gregg disclose the limitations of Claim 16 above. Kalavade further discloses wherein providing user access to the subscription account includes providing user access to a wireless network account (paragraph 0018).

Regarding Claim 18, Kalavade and Gregg disclose the limitations of Claim 17 above. Kalavade further discloses wherein providing user access to wireless network

Art Unit: 2435

account includes providing access to one of a GSM/GPRS network, a 3G network and a Personal Handyphone Network (paragraph 0059).

Regarding Claim 19, Kalavade and Gregg disclose the limitations of Claim 16 above. Kalavade further discloses wherein providing user access to the subscription account includes providing user access to a location-based services account (paragraph 0018).

Regarding Claim 21, Kalavade and Gregg disclose the limitations of Claim 20 above. Kalavade further discloses wherein the network is one of a GSM/GPRS, 3G, Personal Handyphone System (PHS) and a CDMA network (paragraph 0059).

Regarding Claim 22, Kalavade and Gregg disclose the limitations of Claim 20 above. Kalavade further discloses wherein the network is a wireless network (Figure 1, paragraph 0095).

Regarding Claim 23, Kalavade and Gregg disclose the limitations of Claim 20 above. Kalavade further discloses wherein the network is a wired network (Figure 1, paragraph 0095).

Regarding Claim 24, Kalavade and Gregg disclose the limitations of Claim 20 above. Kalavade further discloses wherein the provisioning module, when executed by

the server, further operates to encrypt the SIM secret data to be provided to the computing system (paragraph 0210).

Regarding Claim 25, Kalavade and Gregg disclose the limitations of Claim 24 above. Kalavade further discloses wherein the provisioning module, when executed by the server, further operates to participate in a bilateral key exchange with the computing system over the network (paragraph 0236).

Regarding Claim 26, Kalavade and Gregg disclose the limitations of Claim 20 above. Kalavade further discloses wherein the computing system is further to store the SIM secret data in an encrypted format on a mass storage device of the computing system (paragraph 0217).

Regarding Claim 27, Kalavade and Gregg disclose the limitations of Claim 27 above. Kalavade further discloses wherein the computing system is further to store an encrypted bulk encryption key to be used to decrypt the encrypted SIM secret data (paragraph 0210).

Regarding Claim 28, Kalavade and Gregg disclose the limitations of Claim 28 above. Kalavade further discloses wherein the computing system further includes a hardware token to provide a second key to encrypt the bulk encryption key (paragraph 0198).

Regarding Claim 29, Kalavade and Gregg disclose the limitations of Claim 20 above. Kalavade further discloses wherein the server is further to control access by the computing system to a service (paragraph 0017), upon authorization and authentication of the computing system using the SIM-compliant authentication, authorization and accounting capabilities (paragraph 0261).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is (571)272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/B. N. T./
Examiner, Art Unit 2435
/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435